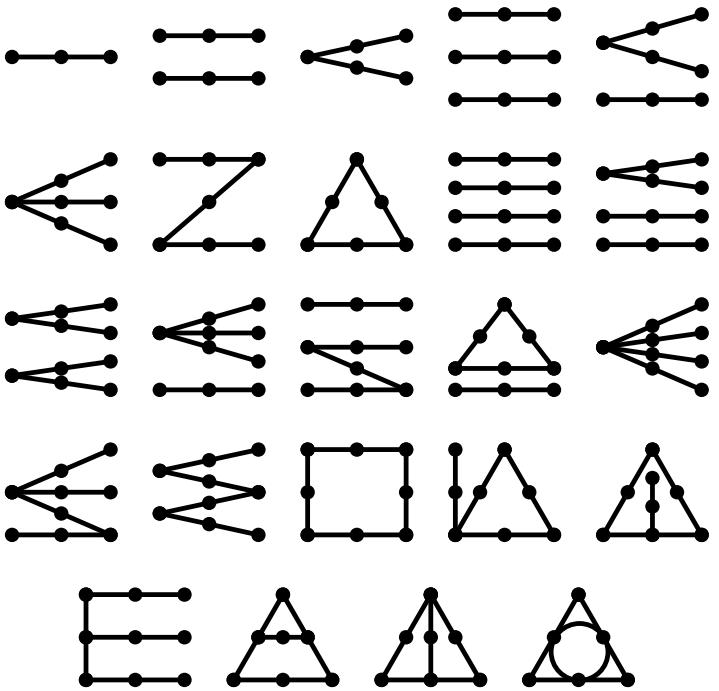
*

ISSN 1350-8539

M500

M500 190



The M500 Society and Officers

The M500 Society is a mathematical society for students, staff and friends of the Open University. By publishing M500 and 'MOUTHS', and by organizing residential weekends, the Society aims to promote a better understanding of mathematics, its applications and its teaching.

The magazine M500 is published by the M500 Society six times a year. It provides a forum for its readers' mathematical interests. Neither the editors nor the Open University necessarily agree with the contents.

MOUTHS is 'Mathematics Open University Telephone Help Scheme', a directory of M500 members who are willing to provide mathematical assistance to other members.

The September Weekend is a residential Friday to Sunday event held each September for revision and exam preparation. Details available from March onwards. Send SAE to Jeremy Humphries, below.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. Send SAE for details to Norma Rosier, below.

Advice to authors. We welcome contributions to M500 on virtually anything related to mathematics and at any level from trivia to serious research. Please send material for publication to Tony Forbes, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation. If you use a computer, please also send the file on a PC diskette or via e-mail. Camera-ready copy can be accepted if it follows the general format of the magazine.

Reciprocals of prime numbers

Dennis Morris

This paper investigates recurring decimals with periods of length $p-1$ digits in the decimal expansions of reciprocals of primes, $1/p$. Primes that generate such $(p-1)$-length periods are known as *full period* primes. Their periods are known as cyclic numbers because they have the interesting property that their digits are cycled around by multiplication; for example,

$$\frac{1}{7} \;=\; 0.(142857);$$

$$2 \cdot 142857 = 285714, \quad 3 \cdot 142857 = 428571.$$

The paper considers the decimal expansions of $1/p$ in positive integer number bases, $B \geq 2$, and for $p \geq 3$.

A terminological inexactitude: In preference to using unfamiliar terminology, the paper uses the term *decimal* to mean an expansion in any number base, not necessarily 10.

The paper draws heavily upon the theory of congruences and, in particular, the concept of primitive roots. The standard results quoted can be found in the books listed at the end.

Notation

Throughout this article we use B to denote the base in which a number is written. Also

a, b, c, ..., n denote non-negative integers;

p and q are reserved for odd prime numbers;

j is restricted to the values $1 \leq j \leq p-1$;

l is reserved to denote $k+1$;

r_n is reserved to denote the nth remainder after a division;

t is reserved for the length (number of digits) of the recurring period of the decimal expansion;

$[x]$ denotes the largest integer less than or equal to x;

$a|b$ means that a divides into b with zero remainder;

$\gcd(a,b)$ denotes the greatest common divisor of a and b;

$\phi(n)$ (Euler's totient function) means the number of integers less than n which are relatively prime to n. An integer a is relatively prime to n if $\gcd(a,n) = 1$.

Known results for prime numbers

(1) The decimal expansion of $1/p$ is either finite or has a recurring period.

(2) The decimal expansion of $1/p$ is finite in number base B if and only if $B \equiv 0 \pmod{p}$.

(3) The length, t, of the period of an infinite decimal expansion of $1/p$ in number base B is given by the *least* positive integral solution of $B^t \equiv 1 \pmod{p}$. This means that full period decimals occur when the least positive integral solution is $t = p - 1$.

(4) Fermat's theorem: $B^{p-1} \equiv 1 \pmod{p}$ unless B is a multiple of p.

(5) If the decimal expansion of $1/p$ is not finite, the length, t, of the period is a divisor of $p - 1$.

(6) Lagrange's theorem. If $d|p-1$, then $x^d \equiv 1 \pmod{p}$ has d solutions.

To whet the reader's appetite, we next take a look at a few decimal expansions of $1/p$ in different number bases. Note the cyclic repetition of period length as the number base increases.

Number base	$\frac{1}{3}$	$\frac{1}{5}$	$\frac{1}{7}$	$\frac{1}{11}$
4	0.(1)	0.(03)	0.(021)	0.(01131)
5	0.(13)	0.1	$0.(032412)_c$	0.(02114)
6	0.2	0.(1)	0.(05)	$0.(0313452421)_c$
7	0.(2)	$0.(1254)_c$	0.1	$0.(0431162355)_c$
8	0.(25)	$0.(1463)_c$	0.(1)	$0.(0564272135)_c$
9	0.3	0.(17)	0.(125)	0.(07324)
10	0.(3)	0.2	$0.(142857)_c$	0.(09)
11	0.(37)	0.(2)	0.(163)	0.1
12	0.4	$0.(2497)_c$	$0.(186A35)_c$	0.(1)
13	0.(4)	$0.(27A5)_c$	0.(1B)	$0.(12495BA837)_c$
14	0.(49)	0.(2B)	0.2	0.(13B65)

(The subscript c indicates a cyclic number in the appropriate number base.)

Finite expansions

LEMMA 1. If p is prime and $B = kp$, the decimal expansion of $1/p$ is $0.k$.

PROOF. This follows immediately from $pk \div p = k$.

For example, with $p = 5$ we have $1/5 = 0.1$ in base 5, $1/5 = 0.2$ in base 10, $1/5 = 0.3$ in base 15, ...

Infinite expansions

We calculate $1/p$ in the general number base $B = pk+j$, where $1 \le j \le p-1$ and $k \ge 0$:

$$\begin{aligned}
&1 \div p = 0, && r_0 = 1,\\
&B \div p = (pk + j) \div p = k, && r_1 = j,\\
&jB \div p = (jpk + j^2) \div p = kj + \left[\frac{j^2}{p}\right], && r_2 = j^2 \bmod p,\\
&r_2B \div p = (r_2(pk + j)) \div p = kr_2 + \left[\frac{jr_2}{p}\right], && r_3 = jr_2 \bmod p,\\
&r_3B \div p = (r_3(pk + j)) \div p = kr_3 + \left[\frac{jr_3}{p}\right], && r_4 = jr_3 \bmod p,\\
&\qquad\qquad \dots && \dots\\
&r_nB \div p = (r_n(pk + j)) \div p = kr_n + \left[\frac{jr_n}{p}\right], && r_{n+1} = jr_n \bmod p.
\end{aligned}$$

The first digit of any recurring period is always k.

The decimal expansion is

$$0.k\left\{kr_1 + \left[\frac{jr_1}{p}\right]\right\}\left\{kr_2 + \left[\frac{jr_2}{p}\right]\right\}\dots\left\{kr_n + \left[\frac{jr_n}{p}\right]\right\},$$

where $r_n = jr_{n-1} \bmod p$. When $j = 1$, this reduces to $1/p = 0.kkk\dots$.

LEMMA 2. (i) If p is prime and $B = pk + 1$, the decimal expansion of $1/p$ is $0.(k)$.

(ii) If p is prime, the only decimal expansion of $1/p$ with a single digit period occurs when $B = pk + 1$.

PROOF. (i) This has been explained, above. (ii) When $t = 1$, $(pk + j)^t \equiv 1 \pmod p$ only when $j = 1$.

For example, with $p = 5$ we have $1/5 = 0.11111\dots$ in base 6, $1/5 = 0.22222\dots$ in base 11, $1/5 = 0.33333\dots$ in base 16, ...

Returning to the decimal expansion

$$\frac{1}{p} \;=\; 0.k\left\{kr_1+\left[\frac{jr_1}{p}\right]\right\}\left\{kr_2+\left[\frac{jr_2}{p}\right]\right\}\ldots\left\{kr_n+\left[\frac{jr_n}{p}\right]\right\},$$

when $j=p-1$, this reduces to

$$\begin{aligned}\frac{1}{p} &= 0.k\left\{k(p-1)+\left[\frac{p^2-2p+1}{p}\right]\right\}\left\{k+\left[\frac{p-1}{p}\right]\right\}\ldots\\ &= 0.k\{k(p-1)+p-2\}\{k\}\ldots,\end{aligned}$$

an infinite decimal of recurring period 2.

LEMMA 3. (i) If p is prime and $B=pk+(p-1)=pl-1$, the decimal expansion of $1/p$ is

$$\frac{1}{p} \;=\; 0.k\{k(p-1)+p-2\}\{k\}.$$

(ii) If p is prime, the only decimal expansion of $1/p$ with a two digit period occurs when $B=pk+p-1$.

PROOF. (i) As above. (ii) When $t=2$, $t(pk+)^t\equiv 1 \pmod p$ has solutions $j=1$ and $j=p-1$. By Lagrange's theorem there are only these two solutions. The first solution (above) occurs when $B=pk+1$ but because $(pk+1)^t\equiv 1 \pmod p$ when $t=1$, this solution gives a period of length one digit. The second solution, when $t=2$, is $B=pk+p-1$.

For example, when $p=7$, we have $1/7=0.050505\ldots$ in number base 6, $1/7$ =2H2H2H... in base 20, $1/7$ =3N3N3N... in base 27. (Here, H represents 17 and N represents 23.)

So, every time $B=pk$, the decimal is finite, every time $B=pk+1$, the decimal has a period of length one, and every time $B=pl-1$, the decimal has a period of length two. These period lengths clearly repeat every p number bases. I propose to use the term p-cycle to refer to the decimal expansions of $1/p$ between number bases $B=pk$ and $B=p(k+1)-1=pl-1$. Clearly, a p-cycle contains p number bases. As examples of such repeating cycles, see the reciprocals 1/3, 1/5, 1/7 and 1/11 in the table above.

LEMMA 4. The fraction 1/5 generates an infinite number of cyclic numbers. These numbers occur in number bases of the form $5k+2$ and $5k+3$.

PROOF. With $p=5$, using $B^t\equiv 1 \pmod p$ and recalling that cyclic numbers occur when least positive solution is $t=p-1$, we have

$$(5k+2)^1 \equiv 2 \pmod 5, \qquad (5k+2)^2 \equiv 4 \pmod 5,$$
$$(5k+2)^3 \equiv 3 \pmod 5, \qquad (5k+2)^4 \equiv 1 \pmod 5$$

and

$$(5k+3)^1 \equiv 3 \pmod 5, \qquad (5k+3)^2 \equiv 4 \pmod 5,$$
$$(5k+3)^3 \equiv 2 \pmod 5, \qquad (5k+3)^4 \equiv 1 \pmod 5.$$

THEOREM 1. The whole (period length) structure of the p-cycle will repeat.

PROOF. Using $B^t \equiv 1 \pmod p$ for any number base $B = pk + j$ we have

$$(pk+j)^m \equiv j^m \pmod p, \qquad (p(k+1)+j)^m \equiv j^m \pmod p.$$

Thus $1/p$ gives rise to a cyclic number in the first p-cycle if and only if it gives rise to an infinite number of cyclic numbers. We might coin the term *cyclic root* to describe p if it so generates cyclic numbers. This term immediately poses the question: Is every prime a cyclic root? The answer is yes, but, before we go into that, let us examine the nature of the way period lengths are distributed throughout the p-cycle of a prime.

The structure of the p-cycle

We begin by examining a table of minimal residues of j^n mod 13. Recall that the period length is given by the least positive solution of the congruence $B^t \equiv (pk+j)^t \equiv j^t \equiv 1 \pmod p$; thus we can read from this table the period length of 1/13 in number base $pk + j$ by looking for the lowest power of j which is congruent to 1.

The congruences of the powers of j mod 13												
	j^1	j^2	j^3	j^4	j^5	j^6	j^7	j^8	j^9	j^{10}	j^{11}	j^{12}
$j=1$	1	1	1	1	1	1	1	1	1	1	1	1
$j=2$	2	4	−5	3	6	−1	−2	−4	5	−3	−6	1_c
$j=3$	3	−4	1	3	−4	1	3	−4	1	3	−4	1
$j=4$	4	3	−1	−4	−3	1	4	3	−1	−4	−3	1
$j=5$	5	−1	−5	1	5	−1	−5	1	5	−1	−5	1
$j=6$	6	−3	−5	−4	2	−1	−6	3	5	4	−2	1_c
$j=7$	−6	−3	5	−4	−2	−1	6	3	−5	4	2	1_c
$j=8$	−5	−1	5	1	−5	−1	5	1	−5	−1	5	1
$j=9$	−4	3	1	−4	3	1	−4	3	1	−4	3	1
$j=10$	−3	−4	−1	3	4	1	−3	−4	−1	3	4	1
$j=11$	−2	4	−5	3	−6	−1	2	−4	−5	−3	6	1_c
$j=12$	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1

For example: The period length of 1/13 in number bases $13k + 3$ is three because j^3 is the lowest power of j in these number bases which is congruent to 1(mod 13). Similarly, the period length of 1/13 in number bases $13k + 6$ is twelve (cyclic) because $j^{12} = j^{p-1}$ is the lowest power of j in these number bases which is congruent to 1 (mod 13).

Several properties of the congruences are apparent.

(i) The only powers which are congruent to 1 (mod 13) are, of course, the powers which are divisors of $p - 1 = 12$; this is one of the standard results (5) stated above.

(ii) Fermat's theorem: $B^{p-1} \equiv (pk + j)^{12} \equiv j^{12} \equiv 1 \pmod{p}$.

(iii) If the exponent, m, of j is a divisor of $p-1$, then there are m ones in the mth column. This is Lagrange's theorem: if $d|p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

The least positive value of the exponent, m, for which $j^m \equiv 1 \pmod{p}$ is, in usual congruence parlance, the order of j; but this is exactly the least positive solution of $B^t \equiv 1 \pmod{p}$; i.e. the length of the decimal period. Further, the values of j for which 1/13 gives a full period decimal have order $p - 1$; they are the primitive $(p - 1)$-th roots of unity, more simply known as the primitive roots of p. This is exactly where cyclic numbers are found. They are found in number bases of the form $pk + j$, where j is a primitive $(p - 1)$-th root of unity.

THEOREM 2. (i) Cyclic numbers are associated with primes p in number bases $pk + j$, where j is a primitive $(p - 1)$-th root of unity.

(ii) Every odd prime number is a cyclic root.

(iii) Every p-cycle of every odd prime has associated with it $\phi(p - 1)$ cyclic numbers.

PROOF. (i) By definition, primitive roots are residues with order $p-1$. But this is precisely what we are looking for when we seek values of t for which $B^t \equiv 1 \pmod{p}$ has no solution less than $t = p - 1$.

(ii) It is a standard result that primitive roots exist in every odd prime modulus.

(iii) It is a standard result that every odd prime has $\phi(p - 1)$ primitive roots.

As with decimal periods of full length, it is also a standard result that the number of decimals with periods of length m in the p-cycle is given by $\phi(m)$, and this is normally how one would calculate such numbers. However, rather than calculate the numbers of such shorter periods by this method,

it is instructive to go about it in a longer way. Let us laboriously calculate the numbers of different period lengths of 1/13 for the number bases 31 to 61.

(i) We know that this decimal is finite in number bases of the form $pk = 31k$. Clearly, there is only one such number base in the range 31 to 61. In number base 31, 1/31 is finite, $1/31 = 0.1$.

(ii) The integers, a, which are less than 30 and have $\gcd(a, 30) = 1$ are 1, 7, 11, 13, 17, 19, 23 and 29. Thus we have: $\phi(p-1) = \phi(30) = 8$. Thus there are 8 full period decimals distributed throughout the range $B = 32$ to 61.

(iii) The divisors of 30 are 1, 2, 3, 5, 6, 10, 15 and 30.

By Lagrange's theorem, there is one solution of $B^t \equiv 1 \pmod{31}$ with $t = 1$; that solution we know from above is in number base $pk + 1 = 32$. So we have a period length of 1 in number base 32.

There are two solutions of $B^t \equiv 1 \pmod{31}$ with $t = 2$; one is in number base 32, and the other we know from above is in number base $pl - 1 = 61$. So in addition to a period length of 1 in number base 32, we have a period length of 2 in number base 61.

There are three solutions of $B^t \equiv 1 \pmod{31}$ with $t = 3$; one is in number base 32, but there is not one in number base 61 because 2 does not divide 3. So we have two periods of length 3.

There are five solutions of $B^t \equiv 1 \pmod{31}$ with $t = 5$. One is in number base 32, but there is not one in number base 61 because 2 does not divide 5, and there is not one in the number bases associated with the three-digit periods because 3 does not divide 5. So we have four periods of length 5.

There are six solutions of $B^t \equiv 1 \pmod{31}$ with $t = 6$. One is in number base 32, one is in number base 61 because $2|6$, two are in number bases associated with three-digit periods because $3|6$. So we have two periods of length 6.

There are ten solutions of $B^t \equiv 1 \pmod{31}$ with $t = 10$. One is in number base 32, one is in number base 61 because $2|10$, four are in number bases associated with five-digit periods because $5|10$. So we have four periods of length 10.

There are fifteen solutions of $B^t \equiv 1 \pmod{31}$ with $t = 15$. One is in number base 32, two are in number bases associated with three-digit periods because $3|15$, and four are in number bases associated with five-digit periods because $5|15$. So we have eight periods of length 15.

We summarize the results in the table below.

Periods of length 1	1	Periods of length 6	2
Periods of length 2	1	Periods of length 10	4
Periods of length 3	2	Periods of length 15	8
Periods of length 5	4	Periods of length 30	8

Thus we able to predict the numbers of different period lengths throughout the p-cycle for any odd prime. Of course, this does not enable us to know in advance of working it out what the period length will be in a given number base. We continue by stating another standard result.

(7) If an integer j has order m modulo p and $b > 0$, then j^b has order $m/\gcd(b, m)$. In our terms this means that if $1/p$ has a period of length m in number base $pk+j$, then in number base $pk+j^b$ it has a period of length $m/\gcd(b, m)$.

We initially seek periods of full length; that is, cyclic numbers with periods of length $m = p-1$. In more technical terms, we seek the primitive roots of p. Assume we have already found a primitive root of p. Let us call it j. We thus have a number base, $pk + j$, in which $1/p$ is a full period decimal. The standard result says that there will be other primitive roots in number bases $pk + j^b$ provided $\gcd(b, p-1) = 1$. The required b are, of course, the $\phi(p-1)$ integers which are relatively prime to $p-1$. Clearly, because j is a primitive root of p and these $\phi(p-1)$ different integers, b, are all less than $p-1$, all j^b will all be mutually incongruent in modulus p. Thus, given one number base in which $1/p$ is a full period decimal, we are able to find all other number bases having full period decimals.

We demonstrate with $p = 31$. We have that $1/31$ is a full period decimal in number base $34 = pk + j$, where $j = 3$; $\phi(p-1) = \phi(30) = 8$. Since 3 is a primitive root of 31, there will be primitive roots of 31 in number bases 3, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29}. These will be at positions in the p-cycle given by $j = 3^b \bmod p$. So $3^1 \equiv 3$, $3^7 \equiv 17$, $3^{11} \equiv 13$, $3^{13} \equiv 24$, $3^{17} \equiv 22$, $3^{19} \equiv 12$, $3^{23} \equiv 11$ and $3^{29} \equiv 21 \pmod{31}$, giving $j = 3$, 11, 12, 13, 17, 21, 22, 24. Thus 31 has cyclic numbers in number bases $31k + j$ for these values of j. Of course, we do not need to restrict ourselves to the search for full period decimals. Decimals of period $(p-1)/2 = 15$ occur in number bases $31k + (3^b \bmod 31)$, where $\gcd(b, p-1) = 2$, and likewise for the other divisors of $p-1$.

In short, given the number base of any one full period decimal, we can calculate the period lengths in every other number base.

Some scraps

LEMMA 5. If j is a primitive root of p then so is j^{p-2}.

PROOF. This follows from $\gcd(p-2, p-1) = 1$.

So primitive roots come in pairs.

LEMMA 6. If j is a quadratic residue of p, $1/p$ is never a full period decimal in number base $pk + j$.

PROOF. If j is a quadratic residue of p, then $j^{(p-1)/2} \equiv 1 \pmod{p}$. Since exactly half of the residues of an odd prime are quadratic residues, it follows that $1/p$ cannot be a full period decimal in more than one half of the number bases in the p-cycle (discounting $B = pk$).

Looking at the congruence table on page 5, we see that (i) even powers are symmetric about the line between $j = (13-1)/2$ and $j = 13-(13-1)/2$; (ii) odd powers are symmetric about the same line except that the signs are reversed.

LEMMA 7. (i) Within a p-cycle, the period length, t, is correlated between number bases $pk + j$ and $p(k + 1) - j$.

(ii) If the length, t, of a period is even both in number base $pk + j$ and number base $p(k + 1) - j = lk + j$, then the period length in these number bases will be the same.

(iii) If the length, t, of a period is odd in number base $pk + j$, then the period length in number base $p(k + 1) - j = lk + j$ is twice this length.

PROOF. (i) The period length in base $pk + j$ is given by the least positive solution, t, of $(pk + j)^t \equiv 1 \pmod{p}$.

(ii) This follows from $(pk + j)^t \equiv j^t \pmod{p}$.

(iii) Similarly, $(p(k + 1) + j)^t \equiv (-1)^t j^t \pmod{p}$.

LEMMA 8. If $p = 2q + 1$, where p and q are odd primes, then half of the values of $2 \le j \le p - 2$ are primitive roots.

PROOF. We have $\phi(2q) = q - 1 = (p - 3)/2$.

References

D. Burton, *Elementary Number Theory.*

G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers.*

E. Weisstein, *Concise Encyclopaedia of Mathematics.*

Solution 187.3 – Square wheels

A car has square wheels. On what sort of road can you drive it and experience a smooth ride?

John Smith

After much algebra, made worse by algebraic errors, I find the equation of the road surface suitable for wheels of side $2a$ seems to be given by sections of catenary of the form

$$y \;=\; a\cosh\frac{x}{a}$$

with $|x| \le a\log(1+\sqrt{2})$, where x is measured horizontally and y is measured downwards.

The best way forward seems to be to work back from the answer, to show that it satisfies the question. To see that this is true, first we show that the centre of the square wheel will remain at a constant height, and second we show that the transitions between sections of curve are just as needed.

Let s be the (curved) distance along the road surface; let ψ be the angle between the horizontal and the tangent to the road surface. Then

$$\begin{aligned} s &= \int \sqrt{1+(y')^2}\,dx \\ &= \int \sqrt{1+(\sinh x/a)^2}\,dx \;=\; \int \cosh\frac{x}{a}\,dx \;=\; a\sinh\frac{x}{a} \end{aligned}$$

and

$$\begin{aligned} \tan\psi &= \frac{dy}{dx} \;=\; \sinh\frac{x}{a}, \\ \cos\psi &= \frac{1}{\sqrt{1+(\tan\psi)^2}} \;=\; \frac{1}{\cosh x/a}, \\ \sin\psi &= (\tan\psi)(\cos\psi) \;=\; \tanh x/a. \end{aligned}$$

When the wheel has rolled a distance s along the road surface, so that the contact point between wheel and road is (x,y), then the centre of the wheel will be at y-coordinate Y, where

$$\begin{aligned} Y &= y - a\cos\psi - s\sin\psi \\ &= a\cosh\frac{x}{a} - \frac{a}{\cosh x/a} - a\sinh\frac{x}{a}\cdot\tanh\frac{x}{a} \\ &= \text{little manipulation} \;=\; 0. \end{aligned}$$

This establishes that the wheel centre remains at a constant height.

If the wheel has rolled a curved distance a along the road (from the top of a lump), then

$$s \;=\; a \quad\Rightarrow\quad \sinh\frac{x}{a} \;=\; 1 \quad\Rightarrow\quad \tan\psi \;=\; 1,$$

so that the wheel has rotated 45 degrees, and hence the wheel centre is directly above the contact point with the road. Also the length of the bits of road is determined by

$$|x| \;<\; a\log(1+\sqrt{2}),$$

which was chosen so that at the road junctions

$$\begin{aligned} s \;&=\; a\sinh\frac{x}{a} \;=\; a\sinh\log(1+\sqrt{2}) \\ &=\; \frac{a}{2}\Big(\exp(\log(1+\sqrt{2})) - \exp(-\log(1+\sqrt{2}))\Big) \\ &=\; \frac{a}{2}\left(1+\sqrt{2}-\frac{1}{1+\sqrt{2}}\right) \;=\; \frac{a}{2}(1+\sqrt{2}-\sqrt{2}+1) \;=\; a, \end{aligned}$$

as required.

If the car is to maintain a constant forward speed, then the rate of rotation of the wheels will not be constant. Will this generate an unfortunate amount of wear on the engine?

What happens with an equilateral triangular or regular pentagonal wheels? Maybe it's obvious, but I haven't thought about it.

Tony Forbes

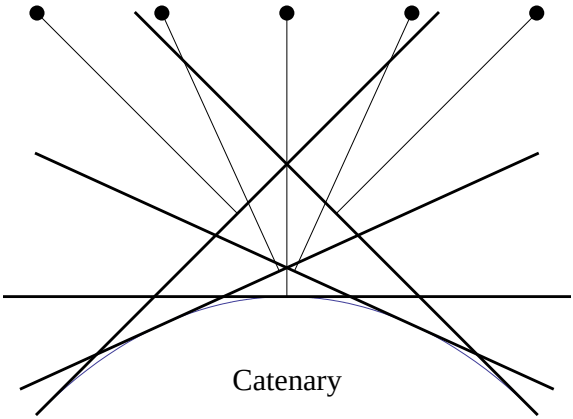
The situation is illustrated by the upper diagram on the next page. The curved part is the catenary.

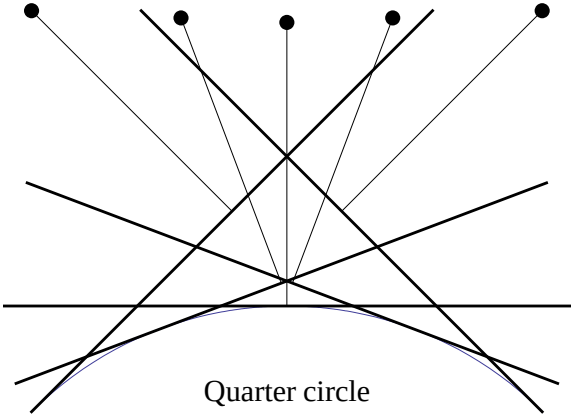
Five positions of the wheel are shown. The tangents correspond to the driving side of the square as the wheel progresses from one trough to the next. The length of the curve is exactly the same as the length of a tangent, $2a$. If you move out distance a at a right angle from the centre of a tangent, you reach the axle of the wheel, indicated by a small black blob. In spite of the complexity of the diagram, isn't it marvellous to see the five blobs neatly arranged in a dead straight line along the x axis?

Martyn Lawrence and **Ralph Hancock** showed that a reasonable approximation to a smooth ride is possible if the humps have a quarter

circle cross-section. The circle has radius $4a/\pi$, and therefore (i) the length of the curved part of each section is $2a$, and (ii) the sections meet at right angles. Unfortunately there is a slight wobble in the height of the axle, as you can see in the lower diagram.

Martyn also wonders how a society where square-wheeled cars are the norm might implement traffic calming measures in residential areas and near schools. He suggests that the effect of 'sleeping policemen' could be achieved by short sections of smooth, flat road.

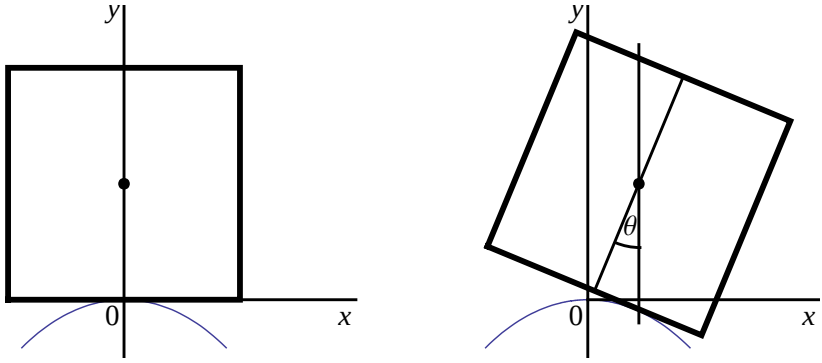




How do you make a catenoid? ...

Brian O'Donnell

This solution is a 'smooth ride' in the sense that the axles remain at the same level. It is not smooth in the sense that the forward motion is alternately accelerating and decelerating for a constant angular velocity of the wheels. A simple mechanism can remove this juddering motion, but if the pre-Flintstones designers of the vehicle were up to the task, I suppose the round wheel would have dawned on them! I start with a square wheel of side 2.



A little reflection will convince that the point of contact has to be vertically below the axle. So the two conditions to be satisfied are $f'(x) = -\tan\theta$ and $f(x) = 1 - \sec\theta$. Thus $\tan\theta = -f'(x) = \sec\theta\tan\theta\, d\theta/dx$, and hence

$$\Rightarrow \quad \int dx \;=\; \int \sec\theta\, d\theta \quad \Rightarrow \quad x \;=\; \log(\sec\theta + \tan\theta) + C.$$

At the origin, $(x,\theta) = (0,0) \Rightarrow C = 0$; hence

$$x = \log(\sec\theta + \tan\theta) = \log(1 - f'(x) - f(x)) \;\Rightarrow\; f'(x) - f(x) = 1 - e^x.$$

Multiplying through by e^x and integrating, we obtain $e^x f(x) = \int (e^x - e^{2x})\, dx$. Therefore $f(x) = 1 - e^x/2 + Ae^{-x}$, and $f(0) = 0 \Rightarrow A = -1/2$. Hence $f(x) = 1 - \cosh x$. When $\theta = \pi/4$, $f(x) = 1 - \sqrt{2} = 1 - \cosh x$, and $x = \operatorname{arcosh}\sqrt{2}$.

By symmetry and periodicity we can now construct the road. For $|x| \le \operatorname{arcosh}\sqrt{2}$, $f(x) = 1 - \cosh x$, and $f(x) = f(x + 2n\operatorname{arcosh}\sqrt{2})$. Finally, I confirm that this is an exact non-slip solution by showing that the arc length from $x = 0$ to $x = \operatorname{arcosh}\sqrt{2}$ is 1. Indeed, the arc length is

$$\int_0^{\operatorname{arcosh}\sqrt{2}} \left(1 + f'(x)^2\right)^{1/2} dx \;=\; \int_0^{\operatorname{arcosh}\sqrt{2}} \cosh x\, dx \;=\; 1.$$

Solution 187.4 – Cots

Show that $\cot\dfrac{\pi}{2n}\cot\dfrac{3\pi}{2n}\ldots\cot\dfrac{(n-2)\pi}{2n}=\sqrt{n}$ for odd n.

Dick Boardman

We start with the familiar addition formula for the tangent,

$$\tan(\alpha+\beta) \;=\; \frac{\tan\alpha+\tan\beta}{1-\tan\alpha\tan\beta}.$$

From this we get

$$\tan(2\alpha) \;=\; \frac{2\tan\alpha}{1-\tan^2\alpha}, \qquad \tan(3\alpha) \;=\; \frac{3\tan\alpha-\tan^3\alpha}{1-3\tan^2\alpha},$$

and so on. After a few steps a pattern emerges. The coefficients are the familiar binomial coefficients except that they alternate between the denominator and numerator, and their signs alternate in pairs. Taking the signs into account, we can arrange the coefficients in Pascal's tangent triangle:

$$\begin{array}{ccccccccccccc}
 & & & & & 1 & & & & 1 & & & \\
 & & & 1 & & & 2 & & & -1 & & & \\
 & & 1 & & & 3 & & & -3 & & & -1 & \\
 & 1 & & & 4 & & & -6 & & & -4 & & 1 \\
1 & & & 5 & & & -10 & & & -10 & & & 5 & & & 1
\end{array}$$

To prove the general case we use de Moivre's theorem,

$$\cos n\alpha + i\sin n\alpha \;=\; (\cos\alpha+i\sin\alpha)^n.$$

If we expand the right hand side using the binomial theorem and equate real and imaginary parts, we get the formulae for $\cos n\alpha$ and $\sin n\alpha$ in terms of powers of $\cos\alpha$ and $\sin\alpha$, from which the formula for $\tan n\alpha$ is easily found:

$$\tan n\alpha \;=\; \frac{n\tan\alpha-{}^nC_3\tan^3\alpha+{}^nC_5\tan^5\alpha-\ldots}{1-{}^nC_2\tan^2\alpha+{}^nC_4\tan^4\alpha-\ldots}.$$

To find the equivalent formulae for $\cot n\alpha$ we use $\cot n\alpha = 1/\tan n\alpha$ and then divide top and bottom by $\tan^n\alpha$. Thus we get

$$\cot n\alpha \;=\; \frac{\cot^n\alpha-{}^nC_2\cot^{n-2}\alpha+{}^nC_4\cot^{n-4}\alpha-\ldots}{n\cot^{n-1}\alpha-{}^nC_3\cot^{n-3}\alpha+{}^nC_5\cot^{n-5}\alpha-\ldots}.$$

Now choose $n\alpha$ an odd multiple of $\pi/2$ so that the left-hand side is zero. Then we use only the denominator and can cancel one $\cot n\alpha$, giving

$$0 \;=\; \cot^{n-1}\alpha - {}^nC_3\cot^{n-2}\alpha + {}^nC_4\cot^{n-5}\alpha - \cdots + {}^nC_{n-1}.$$

Choose n to be odd and note that ${}^nC_{n-1} = n$. This is a polynomial in even powers of $\cot\alpha$. The products of the roots of this polynomial will be n. However, the roots are $\cot^2(m\pi/(2n))$, where m is odd. Taking the square root of this gives the required expression.

John Smith

After much fiddling and experimental calculation, I find that

$$\sin\frac{\pi}{n}\cdot\sin\frac{2\pi}{n}\cdot\cdots\cdot\sin\frac{(n-1)\pi}{n} \;=\; \frac{n}{2^{n-1}}, \tag{1}$$

$$\cos\frac{\pi}{n}\cdot\cos\frac{2\pi}{n}\cdot\cdots\cdot\cos\frac{(n-1)\pi}{n} \;=\; \pm\,\frac{1}{2^{n-1}} \qquad (n \text{ odd}),$$

and by taking the first $(n-1)/2$ terms (the positive ones) we have

$$\tan\frac{\pi}{n}\cdot\tan\frac{2\pi}{n}\cdot\cdots\cdot\tan\frac{(n-1)\pi}{n} \;=\; \sqrt{n},$$

or

$$\cot\frac{(n-2)\pi}{2n}\cdot\cdots\cdot\cot\frac{3\pi}{2n}\cdot\cot\frac{\pi}{2n} \;=\; \sqrt{n}.$$

But how to prove the results of the sines and cosines?

Sine and cosine identities seemed vaguely familiar from old M500s. I looked through past issues, and there, back in **171**, during the consideration of the products of lengths of chords of polygons, is the result (1), proved by considering the product of the magnitude of the roots of the polynomial

$$(z-1)^{n-1} + (z-1)^{n-2} + \cdots + (z-1) + 1 \;=\; 0.$$

Looking at

$$(z+1)^{n-1} + (z+1)^{n-2} + \cdots + (z+1) + 1 \;=\; 0$$

gives the corresponding identity for the product of cosine terms. The required result follows.

So not entirely an original solution, but I think sufficiently complete.

Also solved by **John Bull** and **Jim James**.

Solution 181.2 – Six secs

Show that

$$\sec\frac{\pi}{7}\,\sec\frac{2\pi}{7}\,\sec\frac{3\pi}{7}\,\sec\frac{4\pi}{7}\,\sec\frac{5\pi}{7}\,\sec\frac{6\pi}{7} \;=\; -64$$

and

$$\sec\frac{\pi}{7}+\sec\frac{2\pi}{7}+\sec\frac{3\pi}{7}+\sec\frac{4\pi}{7}+\sec\frac{5\pi}{7}+\sec\frac{6\pi}{7} \;=\; 0.$$

John Reade

As an alternative to the solution already published [Sue Bromley, M500 **183**, p. 13], it is interesting to show that these problems can be done with Chebyshev polynomials.

There are two kinds of Chebyshev polynomials, $T_n(x)$ and $U_n(x)$, defined as follows:

$$T_n(\cos\theta) \;=\; \cos n\theta, \qquad U_n(\cos\theta) \;=\; \frac{\sin(n+1)\theta}{\sin\theta}.$$

The first few polynomials are

$$\begin{array}{lll} T_0(x) = 1, & & U_0(x) = 1, \\ T_1(x) = x, & & U_1(x) = 2x, \\ T_2(x) = 2x^2-1, & & U_2(x) = 4x^2-1, \\ T_3(x) = 4x^3-3x, & & U_3(x) = 8x^3-4x. \end{array}$$

The easiest way to calculate them is to use the recurrence relations

$$\begin{aligned} T_n(x) &= 2xT_{n-1}(x)-T_{n-2}(x), \\ U_n(x) &= 2xU_{n-1}(x)-U_{n-2}(x) \end{aligned}$$

(the same for both!).

For the problem, the operative polynomial is

$$U_6(x) \;=\; 64x^6-80x^4+24x^2-1.$$

The roots of the equation $U_6(x)=0$ are $\cos n\pi/7$, $n=1,\,2,\,\ldots,\,6$, since

$$U_6(\cos\theta) \;=\; \frac{\sin 7\theta}{\sin\theta} \;=\; 0$$

if $\theta = n\pi/7$, $n=1,\,2,\,\ldots,\,6$. Therefore if we substitute $1/x$ for x in $U_6(x)$, we get the polynomial equation whose roots are $\sec n\pi/7$, $n=1,\,2,\,\ldots,\,6$, namely

$$x^6-24x^4+80x^2-61 \;=\; 0,$$

from which we obtain immediately

$$\sum_{n=1}^{6} \sec \frac{n\pi}{7} \;=\; 0, \qquad \prod_{n=1}^{6} \sec \frac{n\pi}{7} \;=\; -64.$$

The moral is that sines and cosines are all very well but when it comes to secs you have to use your initiative!

Solution 187.6 – Iteration

Find an iteration formula for $A^{1/n}$ that generalizes Heron's method for computing square roots.

John Bull

There are many iteration formulae that would work, and which of these would be regarded as the most analogous to Heron's formula is arguable. But here is one possible answer.

Derive Heron's formula from a rearrangement of $a^2 = A$:

$$2a^2 \;=\; A + a^2, \qquad a \;=\; \frac{1}{2}\left(\frac{A}{a} + a\right).$$

Now consider a similar rearrangement of $a^n = A$:

$$na^n \;=\; A + (n-1)a^n, \qquad a \;=\; \frac{1}{n}\left(\frac{A}{a^{n-1}} + (n-1)a\right).$$

This gives the analogous iteration formula for the nth root of A as

$$a \;\to\; \frac{1}{n}\left(\frac{A}{a^{n-1}} + (n-1)a\right)$$

which, of course, also gives Heron's formula for the particular case of $n = 2$.

D. M. Tansey points out that if Heron were familiar with the Newton–Raphson method, that would work just as well. Put $f(a) = a^n - A$ in the iteration formula

$$a \;\to\; a - \frac{f(a)}{f'(a)}.$$

Solution 184.1 – Twelve boxes

There are twelve closed boxes numbered 1, 2, ..., 12. On each turn you throw a pair of dice and you must open closed boxes whose numbers add up to the sum of the numbers shown by the dice. If this is impossible, the game stops and you lose. If you manage to open all the boxes, the game stops and you win. If neither, the game continues. What's the probability of winning?

We have already printed contributions by **Dick Boardman** and **Ron Potkin** in M500 **188**. However, the following solution to this interesting and difficult problem arrived too late for that issue. Also we can take this opportunity to correct an erratic decimal point in Dick's solution: Dick's strategy achieves 34 games out of 10000, not 1000.

John Smith

Resorting to a computer, we can find the optimal strategy and the probability of winning the game.

First we solve the problem, find the probability of winning, for all possible combinations of closed boxes summing to less than some number n, and store the probability of winning for each such combination. Then, given a combination summing to n, a search over combinations summing to $n-2$ gives us the strategy of winning if we throw a 2. Similarly we can solve for throwing a 3, 4, ..., 12, thus solving the problem for the new combination.

Initially we know the probability of winning when all the boxes are open (i.e. probability 1), so we can inductively work up until reaching all boxes closed. How much effort is involved?

All told, there are 12 boxes, so $2^{12} = 4096$ possible combinations of boxes. To solve each combination requires that we search over roughly $11 \cdot 4096/78$ (eleven possible dice throws, and 78 is the sum $1 + 2 + \ldots + 12$), which is about 600 possible combinations. Now $4096 \cdot 600$ is less than 2.5 million, which is not a lot. Thus, with computer run times of a second or so, we find that the the probability of winning if you always do the best thing is 0.003622181. Using 64 bit integers, we can find this as a rational number,

$$275901419419/76169967501312;$$

the denominator is $3^{19} \cdot 2^{16}$.

Actually describing the strategy is not easy. Certainly, as previously suggested, usually you should open fewer big boxes rather than more smaller

boxes. However there are exceptions.

For example, if boxes 5 and 7 are closed, the probability of winning is 0.064815 = 7/108; if boxes 1, 2, and 9 are closed, the probability of winning is 0.044753 = 29/648. Thus if 1, 2, 5, 7 and 9 are closed, and one throws 12, then open 1, 2, 9.

But if boxes 5 and 4 are closed, the probability of winning is 0.129629 = 7/54; if 6, 2, and 1 are closed, the probability of winning is 0.135802 = 11/81. Thus if 1, 2, 4, 5, 6 are closed and one throws 9, then open 4 and 5.

If I can reduce the masses of data that I now have on the optimal move to something worthwhile, and describe it as a strategy, then I will. But at the moment it is just a huge table of what to do next, and largely still inside the machine.

Problem 190.1 – 50 pence

Colin Davies

Starting on his sixth birthday, a child is given 50 pence every day but always in a different combination of coins. The money stops when this is no longer achievable. How old is the child when that happens?

For readers unfamiliar with British currency, what we are asking for is the number of solutions in non-negative integers a, b, c, d, e, f of the equation $a + 2b + 5c + 10d + 20e + 50f = 50$.

Problem 190.2 – Nested roots

Jim James

Given

$$\sqrt{4+\sqrt{4^2+\sqrt{4^3+\sqrt{\cdots+\sqrt{4^n+\sqrt{\cdots}}}}}} = 3,$$

solve

$$\sqrt{4-\sqrt{4^2-\sqrt{4^3-\sqrt{\cdots-\sqrt{4^n-\sqrt{\cdots}}}}}} = ?,$$

where $n \in \mathbb{N}$ and the sequence of nested roots continues indefinitely.

If it is possible to have only 17 different patterns of wallpaper, how is it that all DIY stores have tons of the stuff on display? —Keith Drever

Problem 190.3 – Goat

In view of the success of Problem 186.5 – Horse, as judged by the amount of interest it generated, here is another transcendental farming problem. This time we have a goat.

There is an infinite field (an expanse of grass—not the kind of thing that you would do arithmetic in). The field contains a barn occupying a space in the form of a regular polygon with $2n$ sides of length 1 metre. The goat is tethered to a corner of the barn by a rope of length n metres. What is the area of grass that the goat can reach?

I (ADF) don't have the answer, but I do know that if you divide the area by the radius^2 of the barn and let n tend to infinity, you should get $5\pi^3/6$. For it is the answer to Problem 34.3 – Goat and field II, which we reprinted in M500 **180**. In that version, the barn is a circle of radius 1 metre and the goat is attached to the circumference by a rope of length π metres.

Thanks to **Martyn Lawrence** and **Basil Thompson** for sending in further solutions to the Horse problem. Alas! they were too late to be mentioned in M500 **189**. Both found the correct formula for the area accessible to the horse, as a function of r, the length of the rope,

$$A(r) \;=\; \pi + \phi(r)\cos\phi(r) - \sin\phi(r);$$

$\phi(r)$ is the angle subtended by that part of the grazeable area where the rope is taut. (Draw a diagram, or see Simon Geard's article in M500 **189**.)

The consensus of opinion is that it is impossible to invert $A(r)$ to an expression $r(A)$ involving only elementary functions. Therefore, except for a few special cases, one of which is where $r(\pi-1)=\sqrt{2}$, the solution requires numerical methods. We are also interested in an elegant solution to the circular barn case. Here, I think 'elegant' has to imply that the solution comes out in a natural manner and does not involve hideous integrals of square roots of quadratic functions. It is possible that such a thing does not exist.

Problem 190.4 – Six celebrities

TG

My mum reckons that there must be something special about her birthday. After all, she can say six celebrities that share her birthday. So the question is: How many people would she need to know for there to be a greater than 50 per cent chance of knowing six people with her birthday?

... By pulling its tail. [cat annoyed]

Solution 187.7 – Task

> Normally a computer task takes t seconds to complete. However, in any interval of duration one second while it is running the task will fail with probability p. When the task fails it has to be started again from the beginning. What is the expected total time for a successful completion of the task?

David Hughes

At last, a problem I think I can solve! Let the failures occur independently according to a Poisson process,

$$\mathbb{P}(\text{failure in } (t, t+\delta t]) \;=\; \lambda\delta t + o(\delta t).$$

Then the time between events has an exponential probability distribution function,

$$f(t) \;=\; \lambda e^{-\lambda t}, \qquad \mathbb{P}(T \le t) \;=\; 1 - e^{-\lambda t},$$

with mean $\mu = 1/\lambda$.

If the expected total time is A, say, then

$$A \;=\; \int_0^s (t + A)\lambda e^{-\lambda t}\, dt + \int_s^\infty s\lambda e^{-\lambda t}\, dt.$$

The factor $t + A$ in the first integral corresponds to the failure occurring before time s, where s is the duration of the task, for then the process must be restarted. The second integral applies if the failure occurs after time s. Thus

$$A \;=\; A - (s + A)e^{-\lambda s} + \frac{1}{\lambda}\left(1 - e^{-\lambda s}\right) + se^{-\lambda s} \;=\; \frac{1}{\lambda}\left(e^{\lambda s} - 1\right),$$

or, in the notation of the problem, $A = (e^{pt} - 1)/p$.

As $pt \to 0$, $e^{pt} \to 1 + pt$ and $A \to t$. The presence of p in the denominator as well as in the exponential means that it is more important to fix your computer than shorten the task!

Problem 190.5 – Eight switches

You have a battery, some wire, some light bulbs and eight switches of the simple on–off kind. Design a circuit that allows you control as many lights as possible, in the sense that you can select any single bulb and switch it on while all the others remain unlit. What if you use LEDs instead of bulbs?

Solution 188.2 – Cylinder

Gradually fill a cylindrical container with a liquid. When is the centre of gravity at its lowest point?

Jim James

It is assumed that the cylinder is set vertically upright and remains so as liquid is added to it. Because of the radial symmetry of its cross section, the centres of gravity of the cylinder, its liquid content and the system as a whole then lie along the cylinder axis. All heights in this solution are relative to the inside, upper surface of the cylinder's base and any consistent system of units may be employed for practical applications.

Let w be the weight of they empty cylinder and c the height of its centre of gravity. Let h be the height of the liquid contained within the cylinder. The height of its centre of gravity is then $h/2$, and the weight of the liquid is kh where k is the cross-sectional area of the cylinder multiplied by the liquid density. Let s be the height of the centre of gravity of the system overall; then because all centres of gravity lie along the cylinder axis, $(w + kh)s = wc + kh \cdot h/2$, or

$$s \;=\; \frac{wc + kh^2/2}{w + kh}.$$

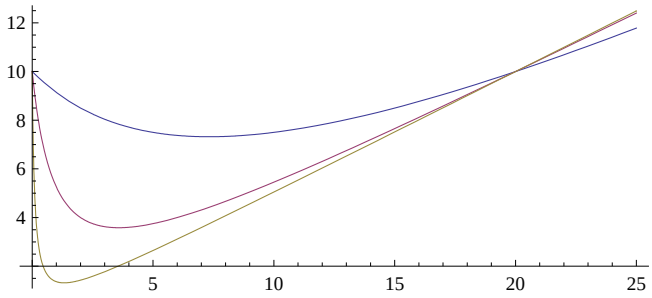
The minimum value of s occurs when $ds/dh = 0$, that is when

$$(wc + kh^2/2)k \;=\; (w + kh)kh, \qquad \text{or} \qquad kh^2 + 2wh - 2wc \;=\; 0.$$

This gives $h = (-w + \sqrt{w^2 + 2kwc})/k$, the positive square root being selected since h can never be negative. Substituting this value of h into the expression for s, the minimum value of s is therefore

$$s_{\min} \;=\; \frac{wc + (A - w)^2/(2k)}{w + (A - w)} \;=\; \frac{2kwc + (A - w)^2}{2kA},$$

where $A = \sqrt{w^2 + 2kwc}$.



The graph illustrates the significance of the magnitude of k in the solution. It shows quantitatively what we expect intuitively: that at liquid levels $h < 2c$ ($= 20$ here), increasing the liquid density and/or the cylinder diameter results in a substantially lower system centre of gravity and hence a more mechanically stable system overall.

Note, too, that all three curves intersect at $h = 2c = 20$. At this point the centres of gravity of the cylinder, liquid content and system are all equal to $c = 10$.

ADF writes — **Colin Davies** observes that there is insufficient data. He says, 'Does not the mass of the cylinder matter? If the cylinder has a mass that is nearly zero, the centre of gravity will go to the bottom immediately after the first few drops of liquid are poured in.' Colin also sent me a cutting from *IEE News* containing an account of various solutions to the problem as it appeared in that publication. In their version, the parameters of the problem, the weight, height and radius of the can, not to mention the density and thickness of the material it was made of, were given in the appropriate SI units. The solutions were presented in the form of numbers to two decimal places and sometimes beyond. However, whilst it might have some appeal to electrical engineers, this was not the kind of answer we were looking for.

I was introduced to the problem during an M202 summer school at Stirling University by that gang of OU tutors, Angela Dean, John Jaworski, John Mason, Alan Slomson, Richard Ahrens, Fred Holroyd and John Kassab, who were known by the name of *Chez Angelique*. At Stirling in the 1970s there was considerable demand amongst mathematics students for something a little more exciting than the usual social activities one normally associates with summer school evenings. Chez Angelique filled that need. It was, simply, an informal gathering to discuss interesting mathematical problems. Sometimes the problems were trivial, sometimes at the cutting-edge of research, but all had in common that element of surprise, beauty, elegance, whatever, that makes our subject worth studying. And to their eternal credit, the hosts did an such excellent job of presenting their nightly material in a delightful and entertaining manner that the impression they made on me lasts to this day, over a quarter of a century afterwards.

Getting back to the cylinder, it turns out that there is indeed an unexpected, 'lateral' way of viewing the problem. Let us look once again at $s_{\min}$, the position of the centre of gravity when it is at its lowest, and $h_{\min}$, the corresponding height of the liquid, recalling that $A = \sqrt{w^2 + 2kwc}$;

$$s_{\min} = \frac{2kwc + (A - w)^2}{2kA}, \qquad h_{\min} = \frac{-w + \sqrt{w^2 + 2kwc}}{k},$$

Before reading on, see if you can spot a likeness between the two expressions.

Yes, you've guessed it, $s_{\min}$ and $h_{\min}$ are identical.

The answer to the problem is that *the centre of gravity is at its lowest when it is coincident with the surface of the liquid.*

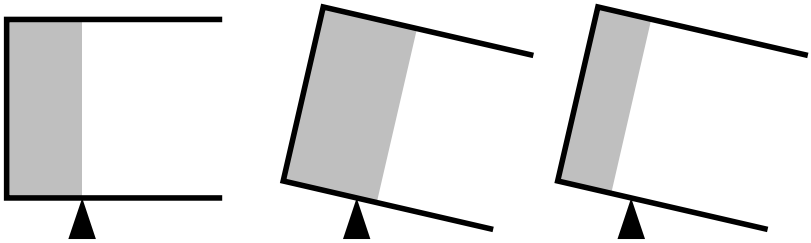
The proof is a simple thought-experiment.

Suppose the centre of gravity is coincident with the surface of the liquid.

Imagine the can tipped on its side and placed on a fulcrum positioned at the level of the liquid surface. (Yes, I admit that this stretches the imagination. As an aside, can you devise an engineering solution to the problem of keeping the liquid from slurping out of the can?)

The can balances. Now add a small amount of liquid. In the diagram, below, the can tips to the right because weight is added to the right of the fulcrum. On the other hand, if we remove some liquid, the system loses weight from the left of the balancing point and, again, the can tips to the right.

Thus in both cases the centre of gravity moves to the right, or upwards when the can is returned to its usual position.



The Stirling summer-school material was collected together and published as *Chez Angelique*, by John Jaworski, John Mason, Alan Slomson *et al.* (1975). If you have it, you might recognize our 'Problem 189.2 – Brown eyes' as a politically corrected version of their 'Forty faithless wives'.

Here's another from the book. Which of these statements are true?

1. Exactly one of these statements is false.
2. Exactly two of these statements are false.
3. Exactly three of these statements are false.
4. Exactly four of these statements are false.
5. All five of these statements are false.

Letters to the Editors

Re: Deniable encryption

Dear Tony,

In my article in M500 **182** I introduced the notion of deniable encryption and claimed that no one had yet devised a suitable encryption algorithm, nor a practical proposal. Actually, there is a way, albeit not a good way. Deniable encryption is feasible but not as would be suitable for general deployment.

Suppose Alice and Bob have devised or procured a hard, near unbreakable, symmetric, private encryption system that takes any size plaintext with any size key. A one-time pad obviously meets the requirement but, given published technology, it would not be difficult to find a more practical alternative. Denote the encryption function as $C = E(P, K)$ where P is the plaintext, K is the key, and C is the encrypted output. Decryption would be achieved with the same function using $P = E(C, K)$.

Now consider the following steps:

1. Alice creates $C = E(P, K)$ and $J = E(D, C)$, where P is a real espionage type of plaintext, D is a dummy compromising message, such as 'Book a room at the Nookie', K is a key shared by Alice and Bob.

2. Alice sends C to Bob.

3. Bob recovers $P = E(C, K)$. Also Bob creates $J = E(D, C)$.

Suppose Alice and Bob have been communicating for some time, with a government agency monitoring the traffic. The cipher is too difficult to break, so the government, supported by the Regulation of Investigatory Powers Act, demands that Alice hand over her key. We assume she would also be required to hand over the encryption algorithm. Rather than hand over K, she hands over J. The government now use J, together with their intercepted ciphertext C, to decipher the message. But rather than recover the real message P, they recover the dummy message $D = E(C, J)$.

There are problems. The key J handed over would need to be different for each message, and moreover each one would be a different size. A standard commercial encryption system generally takes a fixed-size key, usually 128 bits, with the same key used for many messages. An encryption system of this sort would arouse suspicion, especially as it would be much less efficient, by way of processing power and communications bandwidth, than a standard system. Also a different dummy message would be needed each time which, to avoid leaving evidence, would imply meticulous and non-trivial management. Bob may be required to hand over his data, and dummy messages could not be sent over the communications channel, so Alice and Bob would have to build up a bank of dummy messages by prior agreement and synchronize their use.

However, if Alice and Bob were armed with plausible explanations and robust organization, it would be impossible for the authorities to prove that D were not the real intended message.

Given the above method, and the mathematics I demonstrated in previous articles, I suspect there must be a neater way, but so far it eludes me.

John Bull

PS. All of the above is already in the public domain (for example, see Bruce Schneier, *Applied Cryptography*) so I am not revealing anything that could compromise national security.

Calculus

Dear Tony,

When I put into MATHEMATICA 'FullSimplify[TrigExpand[Cot[2Pi/7]]]', it told me that this Cot was the root of a certain polynomial with only even powers and with the constant term of 7. Similarly for 9, 11, 13, etc.

I looked into my copy of *Trigonometric Delights* (reviewed by Barbara Lee in M500 **188**) and found that this polynomial was the denominator in Pascal's tangent triangle and that this solved the problem fairly simply. [See page 14.]

I note that people are still discussing Sebastian Hayes's note, 'Why does calculus work?'. My own view is that in providing a rigorous base for the calculus, the rigorists found it necessary to impose conditions that were only met approximately in the real world, notably that matter was continuous and infinitely divisible rather than molecular and that energy and time were continuous rather than quantized as in quantum mechanics. Calculus works when these approximations are almost valid and tends to fail when we consider molecules or cells or other discontinuous features. These need to be dealt with more like cellular automata.

This is confirmed by looking closely at another book, *The Algorithmic Beauty of Sea Shells*. In this book, Professor Meinhardt produces many of the lovely patterns that appear on sea shells. In the text of his book, he uses many formulae based on partial differential equations but in the program that comes on a disc with the book, the methods he uses are much more akin to cellular automata than true partial differential equations.

Dick Boardman

Venn diagrams

Dear Tony,

I first came across the Venn diagram problem during my early teaching days so I could easily recall the very nice article by Margaret Baron in the *Mathematical Gazette*, vol. LIII, page 113, May 1969, 'A note on the historical development of logic diagrams: Leibniz, Euler and Venn'.

Perhaps you could convey this information to interested colleagues since there is so much more that might be said concerning, for example, the use of lines instead of circles/ellipses for the representation. Perhaps Chris Pile could follow up with a piece based on this article. I'm quite happy to leave it to him!

Bryan Orman

Deux nombres

Dear Tony,

I saw your remarks on the impossibility of 'Deux nombres' [M500 **188**]. Would this help?

If this is about Russian mathematicians, quite likely the original was in Russian. In Russian, the verb 'to be' is often omitted and replaced with a dash (or nothing) whose meaning may be, indifferently, 'it is' or 'they are'. Also, Russian has a genitive case, so 'the sum of two numbers' is 'сумма двух номеров', 'summa dvukh nomerov'. So 'One knows the product and the other the sum of two integers between 2 and 100' might originally have been 'One knows the product, the other the sum of-two of-integers – (= they're) between 2 and 100', where the last part refers to the product and the sum, not to the integers.

Does restricting the product and the sum to between 2 and 100 give a unique solution?

Ralph Hancock

ADF—An interesting suggestion. However, I still can't get a unique answer for any reasonable interpretation of the parameters of the problem. For example, if $2 \le a < b \le 100$, the original solutions are $\{80, 85\}$ and $\{84, 88\}$. However, if we apply the additional constraints $ab \le 100$ and $a + b \le 100$, the solution set changes to $\{\{4, 16\}, \{4, 19\}, \{4, 23\}, \{7, 14\}\}$. Similarly, for $2 \le a \le b \le 100$, pair $\{2, 6\}$ survives, $\{84, 88\}$ is lost and three new ones appear, $\{4, 19\}$, $\{4, 23\}$ and $\{7, 14\}$.

Mathematics in the kitchen – II

Tony Forbes

Following the trend which we started in M500 **188**, here's another scientific experiment that you can perform with materials available in any well-equipped kitchen. As no dangerous procedures are involved there should be no need for any specific safety advice. Nevertheless, we ask you: *please do not do this experiment if you are unwilling to take responsibility for any accidents.*

You will need a kitchen sink, several litres of liquid water and a colander. Again, there is a perplexing mathematical principle the elucidation of which is at present beyond our comprehension. Enlightenment would be much appreciated.

Place the water in the sink. There should be sufficient to submerge the colander, regardless of its orientation in 3-space. Carefully place the colander, right way up, on the surface of the water and let it go.

Water will enter the colander through the holes at the bottom and, not surprisingly, it will descend vertically into the sink. However, after a little while the graceful vertical descent ceases abruptly and the colander tips to one side. Its descent continues in this listed fashion until another mysterious condition arises and then the colander suddenly reverts to its vertical position in which orientation it remains for the remainder of its journey to the bottom of the sink.

Crossnumber solution

1	8	8	9	5	6	8
7	■	■	5	■	■	2
7	■	4	7	3	■	4
1	2	1	■	6	9	2
5	■	3	2	4	■	6
6	■	■	6	■	■	4
1	5	3	5	1	2	1

Tony Forbes writes — I hope it wasn't too difficult. It should come out fairly quickly as soon as you notice that 1-down must be a sixth power. On the other hand, I apologize for the crossnumber in M500 **182**. The story is that I tried it by hand and after about 12 pages of working I was getting nowhere. I therefore began to suspect that it might be unsolvable without the aid of a computer.

So I asked Jeremy for his opinion and I was quite reassured when he told me that he had completed it 'in about 10 minutes'. Presumably I had missed something. Unfortunately, I did not realize that Jeremy was in fact referring to a totally different crossnumber! That one was sent to us by Colin Davies and appeared sometime last year in *IEE News*.

Problem 190.6 – Triangle

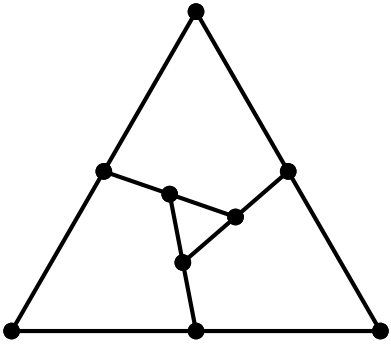
Tony Forbes

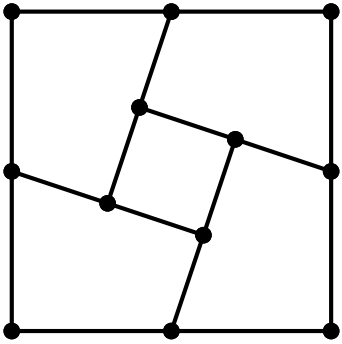
Look at the left-hand diagram (which I found impossible to draw without solving this problem!). The short lines bisect each other as well as the sides of the big triangle. The big triangle is equilateral.

Clearly the small triangle is equilateral. What are the co-ordinates of its vertices?

Devise a ruler-and-compasses construction for the diagram.

Do the same for a square, a pentagon, ... I cannot draw the pentagon because my solution has not progressed beyond the square.





Problem 190.7 – Four roots

Show that if $a^3 > 4b > 0$, the polynomial

$$x^4 - ax^3 + bx - \frac{b^2}{a^2}$$

has four real roots which are in a harmonic ratio.

(I (ADF) found something like this in an old book of problem papers for university entrance examination candidates. I thought it looked interesting, so I offer it to M500. If you do submit a solution, perhaps you can remind the Editor of what it means to be in a harmonic ratio.)

Contents M500 190 – February 2003